May 27, 2016

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106

Dear Ms. Dortch,

The Advanced Communications Law & Policy Institute ("ACLP") at New York Law School respectfully submits the following comments in the above-referenced docket.[1]

* * * * *

1. INTRODUCTION 2
2. A PRIMARY SHORTCOMING OF THE PROPOSED RULES IS THAT THEY DO NOT REFLECT THE TRUE NATURE OF THE DATA COLLECTION UNIVERSE 4
   - 2.1 *General Dynamics* 4
   - 2.2 *The Major Players & Their Motivations* 7
   - 2.3 *The Narrow Role of ISPs in the Data Collection Universe* 13
3. ADDITIONAL INADEQUACIES OF THE FCC PROPOSAL 14
   - 3.1 *Likely Negative Impacts on the Broadband Ecosystem* 14
   - 3.2 *Additional Concerns & Unanswered Questions* 17
4. A MORE PRO-CONSUMER AND PRO-PRIVACY PATH FORWARD 19
5. CONCLUSION 21

[1] The ACLP is an interdisciplinary program that focuses on identifying and analyzing key legal, regulatory, and public policy issues impacting stakeholders throughout the advanced communications ecosystem. For more information, please visit the ACLP's website.

1. INTRODUCTION

The Commission, in its Notice of Proposed Rulemaking (NPRM), seeks to adopt rules that will help Internet users "protect their privacy."[2] This is a worthwhile and essential goal in a digital world dominated by the surreptitious – some say "creepy"[3] – collection and monetization of personal information.[4] Unfortunately, the Commission's proposals are woefully inadequate vis-à-vis bolstering consumer privacy online because they do not reflect the actual contours of the modern digital world. The real power over data – *i.e.,* the ability and incentive to track, collect, aggregate, monetize, and otherwise use customers' personal information to impact and shape their online experience across networks, devices, and applications – is possessed not by Internet service providers (ISPs) but by a vast range of other actors in the ecosystem: search firms, social media sites, content producers, device manufacturers, data brokers, digital advertisers, and other "edge providers."[5] The FCC is right to observe that "broadband networks are not, in fact, the same as edge providers,"[6] but, as discussed at length in these comments, creating a bifurcated regulatory regime for online privacy would nevertheless be harmful.

Why is consistency important? In general, it is increasingly difficult – and ultimately counterproductive – to segment the ecosystem into discrete sectors for regulatory purposes. Therefore, creating two disparate frameworks for online privacy – a prescriptive *ex ante* regulatory regime for ISPs administered by the FCC, and a laxer *ex post* framework

---

[2] *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, at ¶ 2, WC Docket No. 16-106 (rel. April 1, 2016) ("*NPRM*").

[3] *See, e.g.,* Omer Tene and Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 Yale J. L. & Tech. (2013) (observing that "…intuitions and perceptions of how our social values should align with our technological capabilities are highly subjective. And, as new technologies strain our social norms, a shared understanding of that alignment is even more difficult to capture. The word "creepy" has become something of a term of art in privacy policy to denote situations where the two do not line up." *Id.* at 60) ("*Theory of Creepy*"). *See also* Courtney Banks, *Top 10: The Quotable Eric Schmidt*, Jan. 21, 2011, Wall St. Journal Digits Blog, http://blogs.wsj.com/digits/2011/01/21/top-10-the-quotable-eric-schmidt/ (quoting then-Google CEO Eric Schmidt as saying "Google policy is to get right up to the creepy line but not cross it.").

[4] The literature on online data collection and monetization is vast and continues to grow. For an overview of major issues, *see generally* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015) (providing a detailed examination of the many ways in which online companies collect and use data and willfully hide their methods from consumers and regulators) ("BLACK BOX SOCIETY"). For further discussion and examples, *see infra* section 2.

[5] *See, e.g.,* Peter Swire et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less Than Access by Others*, The Institute for Information Security & Privacy at Georgia Tech (Feb. 2016), http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf ("*Swire Study*"). It should be noted that ISPs might also one day engage in similar kinds of behavior, but their current business models continue to revolve primarily around subscriptions to voice, video, and data offerings. *See Letter from National Associations to the Honorable Tom Wheeler*, Feb. 11, 2016, http://www.ctia.org/docs/default-source/fcc-filings/021116-privacy-letter.pdf (arguing that regulatory parity is necessary so that ISPs can explore ways of "provid[ing] their customers new products and customized services").

[6] *NPRM* at ¶ 4.

for edge providers administered by the FTC – would likely create confusion among consumers and create significant arbitrage opportunities for less regulated edge firms.

The potential for consumer harm stemming from this approach is palpable. Evidence suggests that consumers are wary but generally accepting of some level of data collection and usage.[7] Their comfort, however, is situation-specific, rendering it futile to impose rules applicable to only one set of actors in the broadband ecosystem.[8] This dynamic is compounded in a world where data collection is pervasive, incentives to "use and share extensive and personal information" about consumers are universal,[9] and many firms exert some level of control over a user's information and online experience.[10] Accordingly, applying disparate levels of regulatory scrutiny to different segments of the ecosystem will inevitably skew consumer expectations for privacy protections – expectations that won't be met in a uniform manner under a bifurcated regulatory framework governing online privacy. Consumers wishing to hold their search engine, favorite social media service, or handset manufacturer to the same privacy standards as their ISP, for example, will find themselves without recourse. Rather than "encourage use of broadband networks," this dynamic could chill it, thus undermining rather than bolstering the "virtuous cycle" of investment in broadband networks and the services that are enabled by them.[11] There are also real concerns about the likely negative impacts of this approach on the ability of ISPs to explore new revenue streams and continue investing at high levels in their services over the long term.[12]

To assure truly pro-consumer and pro-privacy outcomes, these comments respectfully urge the Commission to reevaluate its proposal and consider an alternative path forward – a path that is grounded in foundational notions of parity, neutrality, clarity, consistency, and humility:

- Unless and until there is evidence of *actual* consumer harms stemming from the collection and misuse of personal information by ISPs, the Commission should forbear from applying any new or existing privacy rules under section 222. This would mirror at a very high level the *ex post* framework for online privacy that the FTC currently maintains for edge providers.

---

[7] *See generally* Lee Rainie and Maeve Duggan, *Privacy and Information Sharing*, Pew Research Center (Jan. 2016), http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf (finding that, overall, "Most Americans see privacy issues in commercial settings as contingent and context-dependent.") ("*Privacy and Information Sharing*").

[8] *Id.*

[9] *NPRM* at ¶ 3.

[10] *See generally Swire Study*.

[11] *Cf. NPRM* at ¶¶ 11, 309.

[12] *See, e.g.,* Emily Field, *Moody's Says FCC Internet Privacy Rules Could Hurt ISPs,* March 15, 2016, Law360.com, http://www.law360.com/articles/771825/moody-s-says-fcc-internet-privacy-rules-could-hurt-isps (summarizing an analysis by Moody's Investors Service) ("*Moody's Says*").

- In an effort to demonstrate true leadership on these issues and realize the most optimal outcome for consumers, the FCC should call on Congress to step in and identify the broad outlines of a federal digital privacy regime. Congressional action is needed to clarify the regulatory treatment of broadband Internet access service and reconcile the jurisdictional mandate of the FCC and FTC with respect to policing the data collection practices of all firms in the ecosystem. Only a unified approach to privacy protection will bolster consumer welfare.

- If the Commission elects to move forward with some version of the privacy rules proposed in the NPRM, then it should apply them across the entire ecosystem in order to assure consistency, parity, and truly robust consumer protection. The FCC appears to have legal authority to extend its reach to edge providers according to its expansive interpretation of section 706. Ultimately, uniformly applied privacy rules will have an even greater impact on consumer use of online services than the Commission's current proposal, an outcome that would greatly enhance the virtuous cycle of investment and use in the broadband ecosystem.

2. A PRIMARY SHORTCOMING OF THE PROPOSED RULES IS THAT THEY DO NOT REFLECT THE TRUE NATURE OF THE DATA COLLECTION UNIVERSE

A major failing of the NPRM is that it presents an incomplete picture of the complex tapestry that is online data collection. By focusing just on ISPs, the Commission shines only a narrow sliver of light on a very small portion of what has become a massive industry built on the mining and monetization of personal information gleaned from consumers' online activities. A better approach would be to aim a spotlight on this space and develop policies and protections that accurately reflect the true nature of the ways in which firms vie for the acquisition of more granular consumer information. The FTC did this when it grappled with understanding the business models and methods by which "commercial entities…collect or use consumer data."[13] Importantly, it recognized the need for Congressional intervention to enshrine basic protections. Failure by the FCC to be as comprehensive and thoughtful – in the form of a preliminary Notice of Inquiry, public workshops, working with Congress, and/or other efforts to engage experts and call for legislative guidance – is inexcusable and should call into question the efficacy of the current proposal.

2.1 *General Dynamics*

Unlike at any time in the past, the business models of modern communications and media firms are increasingly built around collecting and monetizing granular, real-time

[13] *See Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, at vii, FTC Report (March 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf ("*FTC Privacy Report*").

information detailing every aspect of online use.[14] Indeed, this kind of data is the common thread linking together firms throughout the ecosystem.[15] At a very basic level, it is central to what these various firms do: ISPs deliver data to consumers (they derive almost all of their revenue from voice, video, and data subscriptions); content producers create data for delivery to and consumption by consumers (these companies typically make money by placing ads based on these uses); and device manufacturers produce the hardware that consumers can use to access data (in many instances, these firms collect data, too). But in the context of discussions about privacy, this simple schematic is ultimately misleading because it obscures a basic truth about the modern digital ecosystem: firms across every segment, but especially those at the edge, are competing viciously to be the entity that controls how users' data are collected and monetized.[16]

This general dynamic has been evident since the earliest days of the commercial Internet, when firms competed to serve as exclusive portals to Internet content. This "walled garden" approach, however, quickly fell out of favor as consumers took advantage of new tools to explore the World Wide Web.[17] The result was a remaking of the Internet ecosystem: "those who wanted to reach [consumers who were now actively exploring the Web on their own], such as commercial merchants and advertising-driven content providers, found it easier to set up outposts there [in cyberspace] than through negotiated gates of the proprietary services."[18] Accordingly, online firms began to compete for market share in what was a burgeoning e-commerce space.

A major shift occurred when entities assisting consumers in the navigation of this vast new universe of content – primarily search firms – realized that advertisers were willing to pay more for ads that were actually clicked on by customers. This in turn resulted in an arms race among firms trying to develop algorithms and other approaches that could place online ads that were relevant to individual users.[19] This necessitated the development of platforms that could attract users and goad them into sharing more information about

---

[14] *See, e.g.,* James Grimmelmann, *The Structure of Search Engine Law*, 93 Iowa L. Rev. 1, 11-15 (2007) (discussing the role of data in enabling the business models of online search engines).

[15] *See, e.g.,* FRED VOGELSTEIN, DOGFIGHT: HOW APPLE AND GOOGLE WENT TO WAR AND STARTED A REVOLUTION 183-202 (2013) (providing an example of how technological convergence is driving the race to position proprietary platforms like Apple's mobile devices as the primary arbiter of the online experience)

[16] *See, e.g.,* Bryan Choi, *The Anonymous Internet,* 72 Maryland L. Rev. 501 (2013) (discussing the interplay between innovation – or "generativity" – and notions of privacy like anonymity and noting that the robustness of the former increasingly hinges on flexibility in the latter).

[17] *See, e.g.,* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 29 (2008) ("Consumer accessibility to Internet-enabled applications, coupled with the development of graphic-friendly World Wide Web protocols and the PC browsers to support them…marked the beginning of the end of proprietary information services [i.e., walled gardens].").

[18] *Id.*

[19] *See, e.g.,* JOHN BATTELLE, THE SEARCH: HOW GOOGLE AND ITS RIVALS REWROTE THE RULES OF BUSINESS AND TRANSFORMED OUR CULTURE (2006) (providing a detailed overview of how this aspect of the online market evolved in the late 1990s and early 2000s).

themselves – either directly (*e.g.*, by filling out a form or buying a product), indirectly (*e.g.*, by typing in search terms), or surreptitiously (*e.g.,* by tracking users with cookies).

Google spearheaded this fundamental shift in Internet economics. While it was not the first firm to develop an effective algorithm for sorting search results or enter the online advertising business, it produced an incredibly effective integrated system for doing both.[20] Ever since, a growing number of companies throughout the ecosystem have eagerly sought to compete for some part of the online advertising market, which has grown from an industry that generated $9.6 billion in revenues for firms in 2004 (the year of Google's IPO) to one that neared $60 billion in revenues in 2015.[21] The dominant format for digital ads is now mobile, revenue from which has grown at a compound annual rate of 100% since 2010.[22] Google and Facebook dominate this space.[23] Search ads remain a popular format, but non-mobile ad revenue has only grown at a 9% annual rate over the last five years.[24] Google remains the leading firm in search ads in the U.S. and globally.[25]

These structural shifts in the economics underlying many Internet businesses have had profound impacts on personal privacy. In particular, they have created a self-reinforcing cycle of data generation and collection on the one hand and the provision and consumption of targeted services on the other. Consumers, although generally aware of the privacy risks implicated by this general dynamic and wary of certain types of intrusive practices, continue to consume these services and provide, knowingly or not, the increasingly granular data that is necessary to foster continued investment and experimentation by these firms.[26] The result is a race among online firms of all kinds to create new ways for collecting ever-more detailed information and use that data to micro-target services, advertisements, and other online offerings.

---

[20] *Id. See also* Greg Lastowka, *Google's Law*, 73 Brook. L. Rev. 1327, 1335-1351 (2008) (discussing the development of these components of Google's business model).

[21] *See IAB Internet Advertising Revenues Report: 2015 Full Year Results,* at 4, Interactive Advertising Bureau (April 2016), http://www.iab.com/wp-content/uploads/2016/04/IAB-Internet-Advertising-Revenue-Report-FY-2015.pdf ("*2015 IAB Report*").

[22] *Id.* at 7.

[23] *See AOL, Millennial Face Uphill Battle to Capture Mobile Ad Dollars*, Sept. 8, 2015, eMarketer, http://www.emarketer.com/Article/AOL-Millennial-Face-Uphill-Battle-Capture-Mobile-Ad-Dollars/1012954.

[24] *2015 IAB Report* at 7.

[25] *See Google Will Take 55% of Search Ad Dollars Globally in 2015*, March 31, 2015, eMarketer, http://www.emarketer.com/Article/Google-Will-Take-55-of-Search-Ad-Dollars-Globally-2015/1012294.

[26] To get a sense of how consumer attitudes have evolved over time, *compare* Lee Rainie et al., *Anonymity, Privacy, and Security Online,* Pew Internet & American Life Project (Sept. 2013), http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf, *with Privacy and Information Sharing.*

2.2 *The Major Players & Their Motivations*

The lure of commoditizing and monetizing Internet usage data is not confined to search firms like Google or social media entities like Facebook. Although these companies dominate the lucrative market for online advertising, there has been increased experimentation in recent years by a broad array of firms interested in entering this space and positioning themselves as the primary – or exclusive – mediator of the online experience and thus the sole harvester of the personal data that is generated. Consequently, there are few places in today's society where some entity is not trying to extract data from consumers:

- Any computing device linked to the Internet – a laptop used at home; a desktop used at work; a smartphone used on the go – generates data that can be collected by a range of firms, including an operating system (*e.g.,* Apple iOS); web browser (*e.g.,* Google Chrome); search engine (*e.g.,* Bing); data broker (*e.g.,* Acxiom); and content provider (*e.g.,* YouTube).

- A range of new "smart, connected products" – from cars to washing machines – leverage sensors and other communications technologies to generate vast amounts of data that assist in optimizing particular services and that provide more granular insights into individual and aggregate consumer behavior.[27]

- Ad-supported Wi-Fi networks that blanket large areas in cities across the country rely on the data collected from users and passersby to demonstrate value to firms wishing to precisely target ads.[28] Larger billboards are also increasingly leveraging similar kinds of data to ensure that a particular advertisement is relevant in a given area.[29] And in addition to tracking online purchases, many large retailers also track in-store shopping and buying

---

[27] *See, e.g.,* Michael E. Porter and James E. Heppelmann, *How Smart, Connected Products Are Transforming Competition,* Harvard Business Rev. (Nov. 2014), https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition.

[28] *See, e.g.,* Craig Campbell, *LinkNYC Kiosks Provide Free Internet, But For a Price*, Feb. 9, 2016, Gov. Tech., http://www.govtech.com/dc/articles/LinkNYC-Kiosks-Provide-Free-Internet-But-for-a-Price.html (summarizing privacy concerns stemming from a citywide Wi-Fi network being deployed in New York City); Benjamin Dean, *The Heavy Price We Pay for 'Free' Wi-Fi,* Jan. 25, 2016, The Conversation, https://theconversation.com/the-heavy-price-we-pay-for-free-wi-fi-52412 (articulating an array of concerns regarding the quid pro quo involved in providing "free" online services in exchange for the collection of granular personal information).

[29] *See, e.g.,* Grant Gross, *Billboards Can Track Your Location, and Privacy Advocates Don't Like it*, March 3, 2016, CSO, http://www.csoonline.com/article/3040607/security/billboards-can-track-your-location-and-privacy-advocates-dont-like-it.html.

habits of customers by tapping into data emanating from their smartphones.[30]

- An emerging class of in-home devices like smart TVs and Amazon's Echo actively listen to consumers, gather relevant information, and respond to commands to purchase new products, change the channel, or search for the answer to a question.[31] Similarly, a new and emerging line of wearable products – smart watches, smart glasses and contacts, etc. – are being positioned as real-time portals into personal health data and other metrics that could help companies develop even more detailed portraits of users.[32] Smart cars are also a growing locus of data generation and collection.

- The continued improvement of artificial intelligence, the foundation upon which many of these new "smart" products is built, relies on a constant stream of new data in order to improve the underlying algorithms and make them more useful and responsive to consumer interactions.[33]

The ability to generate these new kinds of data flows about a consumer's online and offline uses has further intensified the rivalry among online firms that depend on advertising revenues stemming from the monetization of customer data. Because these new bits of information tend to be diffused across a number of disparate devices, networks, applications, and locations, these firms are focused on building platforms that can span these various uses and tie the data together more cohesively. In many ways, this presages a new era of "walled gardens," where online firms seek to serve as the exclusive portal through which users navigate nearly all online services. To these ends, the efforts of a company like Google are illustrative of the lengths to which companies are going to monopolize data collection.

At its core, Google is a digital advertising company that possesses enormous power over the online experience. Its business is built around algorithms that place ads that are relevant to consumers who use its services. In 2015, the vast majority of its $74.5 billion in

---

[30] *See, e.g.,* Erin Griffith, *Consumers Hate In-Store Tracking (But Retailers, Startups and Investors Love it)*, March 24, 2014, Fortune, http://fortune.com/2014/03/24/consumers-hate-in-store-tracking-but-retailers-startups-and-investors-love-it/.

[31] *See, e.g.,* Rory Carroll, *Goodbye Privacy, Hello 'Alexa': Amazon Echo, the Home Robot Who Hears it All,* Nov. 21, 2015, The Guardian, https://www.theguardian.com/technology/2015/nov/21/amazon-echo-alexa-home-robot-privacy-cloud ("*Goodbye Privacy*").

[32] *See, e.g.,* Olga Kharif, *Coming Soon to Your Smartwatch: Ads Targeting Captive Eyeballs*, May 12, 2015, Bloomberg, http://www.bloomberg.com/news/articles/2015-05-12/coming-soon-to-your-smartwatch-ads-targeting-captive-eyeballs.

[33] *See, e.g.,* Brian Feldman, *The Future of Tech is Artificial Intelligence and That's Just Fine for Google*, May 18, 2016, New York Magazine, http://nymag.com/selectall/2016/05/googles-back.html.

revenue – over 90% – stemmed from advertising.[34] Its ability to gather user information is extraordinary due to the popularity of services like Google search, Gmail, and YouTube, as well as its assiduous development and acquisition of digital ad technologies and algorithms. In short, Google is everywhere online: according to one recent study, the top five most common online tracking tools are owned by Google, allowing it to "build up detailed profiles on individuals as they move around the Web, assigning them unique identifiers so they can be recognized again."[35] Even after attempting to diversify and reorganizing as a holding company, many of its ancillary businesses involve, to some degree, an effort to get consumers to feed more data into Google's ad machine:

- *Android,* its mobile operating system (OS), is the most popular mobile OS in the world. Google makes Android freely available to handset manufacturers, but it typically mandates that its own apps and services – like Search and Maps – be installed as a default and given priority placement on mobile screens.[36] This type of behavior has provoked significant antitrust scrutiny in Europe;[37] many in the U.S are calling for similar inquiries.[38]
- *Brillo* is an emerging operating system for the Internet of Things (IoT) that is being positioned as a platform across which different devices can communicate and send information.[39] This will provide Google with a unique window into the ocean of information expected to be generated by the IoT.[40]

---

[34] *See* Kris Carlon, *Google Makes One Third of All Global Ad Revenue, But There's Trouble Ahead*, March 18, 2016, Android Authority, http://www.androidauthority.com/google-makes-one-third-global-online-ad-revenue-680883/ (reporting that Google's 2015 total ad revenue was $67.39 billion); Andrews Martonik, *Google Announces Q4 and FY 2015 Earnings: $74.5 billion in Revenue for the Year, $21.2 billion for Q4,* Feb. 1, 2016, Android Central, http://www.androidcentral.com/google-releases-q4-and-full-2015-earnings (reporting that Google's total revenue in 2015 was $74.5 billion).

[35] *See* Tom Simonite, *Largest Study of Online Tracking Proves Google Really is Watching Us All,* May 18, 2016, Technology Review, https://www.technologyreview.com/s/601488/largest-study-of-online-tracking-proves-google-really-is-watching-us-all/.

[36] *See, e.g.,* Amir Efrati, *Google's Confidential Android Contracts Show Rising Requirements*, Sept. 26, 2014, The Information, https://www.theinformation.com/Google-s-Confidential-Android-Contracts-Show-Rising-Requirements.

[37] *See* Mark Scott, *E.U. Charges Dispute Google's Claims That Android is Open to All*, April 20, 2016, N.Y. Times, http://www.nytimes.com/2016/04/21/technology/google-europe-antitrust.html.

[38] *See, e.g.,* Nancy Scola, *Sources: Feds Taking Second Look at Google Search,* May 11, 2016, Politico, http://www.politico.com/story/2016/05/federal-trade-commission-google-search-questions-223078 (reporting on recent inquiries made by the FTC).

[39] *See* Ross Miller, *Google Announces Brillo, An Operating System for the Internet of Things*, May 28, 2015, The Verge, http://www.theverge.com/2015/5/28/8677119/google-project-brillo-iot-google-io-2015.

[40] For recent estimates of data traffic growth expected to be caused by the IoT, *see* Parker Thomas, *Cisco's Traffic Forecast: Growing Opportunity for IoT Enterprises*, Nov. 2, 2015, Market Realist, http://marketrealist.com/2015/11/ciscos-traffic-forecast-growing-opportunity-iot-enterprises/.

- *Chrome* is Google's proprietary Internet browser, which is also available for use on mobile devices and as an operating system for Chromebook laptops. Chrome collects a significant amount of user data in order to enhance the user experience and to assist in refining ad placement.[41]
- *Chromecast*, which also runs on Chrome, lets consumers turn their television sets into smart TVs that support streaming video and other services. This is yet another example of Google attempting to "turn as many devices and screens as possible into ones locked into the company's ecosystem, keep users loyal to that same ecosystem of sites, service and apps, and entice others to join them."[42]
- *Fiber* has played a role in hastening deployment of gigabit-speed broadband networks across the country, an outcome that will benefit Google immensely in the form of more data flowing to its services and thus better visibility into ads that will resonate with consumers.[43]
- *Nexus* phones and tablets also use Android and steer users to Google's own services.
- *Home*, a forthcoming device that incorporates Google's new digital assistant technology, extends its ability to gather further insights into consumers' behavior at home. More broadly, though, Home is a way for Google to bolster the prominence of its new digital assistant (akin to Apple's Siri and Microsoft's Cortana), which is key to helping the company enhance its data collection abilities across multiple platforms: "use our smartphones, tablets, smartwatches, computers and other devices throughout the day, and the Google assistant will be most useful as it follows us around, building a profile on us from interacting with it many times during the course of the day."[44]
- *Loon* is an international connectivity project that seeks to bring more people online and thus using Google services: "…in addition to Google's professed desires to help the world, the economics of ad-supported Web businesses give the company other reasons to think big. It's hard to find new customers in Internet markets such as the United States. Getting billions more people

---

[41] *See* Google Chrome, Privacy White Paper (April 2016), https://www.google.com/chrome/browser/privacy/whitepaper.html.

[42] *See* Gregg Keizer, *With Chromecast, Google Reveals Chrome as its Strategic Big Gun*, July 29, 2013, Computer World, http://www.computerworld.com/article/2484445/internet/with-chromecast--google-reveals-chrome-as-its-strategic-big-gun.html.

[43] *See, e.g.,* Brian Fung, *Google Fiber's Targeted TV Ads are Just the Start of a Bigger Revolution in Advertising,* March 24, 2015, The Switch Blog, Wash. Post, https://www.washingtonpost.com/news/the-switch/wp/2015/03/24/google-fibers-tv-ads-will-soon-know-who-you-are-and-thats-just-the-start/.

[44] *See* Jan Dawson, *Echo and Home are Endpoints, Not End Games*, May 23, 2016, Re/Code, http://www.recode.net/2016/5/23/11746156/amazon-echo-google-home-virtual-assistant-rivals.

online would provide a valuable new supply of eyeballs and personal data for ad targeting."[45]

- *Maps* is an ambitious effort to map the world and use the GPS installed in mobile devices to provide consumers with accurate directions. It is also a way for the company to use personal information to steer users to particular locations that pay to promote their businesses on the map.[46]
- Google's work on *self-driving cars* could position it as a primary conduit for the massive amount of data likely to be generated from constantly monitoring a vehicle and what the passengers inside are doing. In addition, the cars themselves will feed road and traffic data into services like Maps and Waze. More broadly, this fits into a longstanding Google strategy: "Google wants to make the physical world legible to robots, just as it had to make the web legible to robots (or spiders, as they were once known) so that they could find what people wanted in the pre-Google Internet of yore."[47]
- *Sidewalk Labs* has invested in an ad-supported Wi-Fi network in New York City, which is expected to generate hundreds of millions of dollars in advertising revenue over the next few years.[48] This is part of the company's broader efforts to support "smart city" services, which will generate a significant amount of new data stemming from nearly every aspect of municipal life and city government.[49]
- *Wallet* was launched in an effort to provide consumers with a central platform for purchasing goods. A key part of this strategy was Google's desire to gather data from and about consumers – both directly and from the banks that enabled these transactions – so it could more precisely target relevant ads.[50]

---

[45] *See* Tom Simonite, *10 Breakthrough Technologies 2015: Project Loon*, Technology Review, https://www.technologyreview.com/s/534986/project-loon/.

[46] *See* Tom Mendelsohn, *Google Maps Goes Down Scenic Route with Ad-Heavy "Promoted Pins*," May 25, 2016, Ars Technica, http://arstechnica.com/business/2016/05/google-maps-ads-promoted-pins-location/.

[47] *See* Alexis C. Madrigal, *The Trick that Makes Google's Self-Driving Cars Work*, May 15, 2015, The Atlantic, http://www.theatlantic.com/technology/archive/2014/05/all-the-world-a-track-the-trick-that-makes-googles-self-driving-cars-work/370871/.

[48] *See, e.g.,* Alex Davies, *Google's City-Fixing 'Sidewalk Labs' is Finally Getting to Work*, Feb. 23, 2016, Wired, https://www.wired.com/2016/02/googles-city-fixing-sidewalk-labs-is-finally-getting-to-work/.

[49] *Id.*

[50] *See, e.g.,* Tim Bajarin, *Why Google Wallet Has Been a Failure,* Sept. 29, 2014, PC Mag., http://www.pcmag.com/article2/0,2817,2469362,00.asp.

- The company is also competing in the market for *wearables* with offerings like Android Wear, failed efforts like Google Glass, and research into products like smart contacts and virtual reality.[51]

Some have described this expansive approach to monopolizing the collection of user data as a "Trojan horse strategy" whereby the company "hand[s] out free candy with data-mining strings attached."[52] Accurate or not, this description reflects a calculated strategy by Google to diversify its offerings in an effort to acquire some measure of dominance in the race to gather data across the myriad of platforms, devices, services, and networks that now litter and define the ecosystem.[53]

Google is not alone in pursuing this kind of strategy. A major rival in many of these segments is Facebook, a business that is also built around leveraging its user base to generate advertising revenue. Indeed, even though the average Facebook user already spends 50 minutes each day using the social media platform and other applications owned by the company (including Instagram and Messenger) – a significant amount of time relative to other daily and online pursuits – it, like Google, is singularly focused on creating a quasi-walled garden environment in an effort to dominate even more of a user's time so it can "learn more about its users – their habits and interests – and thus better target its ads.[54] These motivations have driven the firm to engage in partnerships and endeavors focused on offerings as disparate as real-time news; live video; virtual reality; and, like Google, an initiative to connect billions of non-Internet users across the globe. Recently, Facebook announced its intention to broaden its advertising efforts even further by "collect[ing] information about all Internet users, through "like" buttons and other pieces of code present on Web pages across the Internet. It will then use the information it collects to target ads to non-Facebook users."[55]

Different motivations drive other competitors. Apple and Amazon are major forces in the data collection business, but neither depend on advertising revenues to drive growth, at

---

[51] *See, e.g.,* David Goldman, *Google Wants to Inject Cyborg Lenses into Your Eyeballs*, May 4, 2016, CNN Money, http://money.cnn.com/2016/05/04/technology/google-lenses/index.html?iid=ob_homepage_tech_pool (reporting on research into smart contact lenses).

[52] *See* Leo Sun, *Audi CEO: Google Inc. Could Turn Driverless Cars Into Data Miners*, June 15, 2015, Motley Fool, http://www.fool.com/investing/general/2015/06/15/audi-ceo-google-inc-could-turn-driverless-cars-int.aspx.

[53] *See, e.g.,* Serdar Yegulalp, *Google's Next Act: Diversify and Conquer,* May 20, 2013, Info World, http://www.infoworld.com/article/2614443/techology-business/google-s-next-act--diversify-and-conquer.html.

[54] *See, e.g.,* James B. Stewart, *Facebook Has 50 Minutes of Your Time Each Day. It Wants More*, May 5, 2016, N.Y. Times, http://www.nytimes.com/2016/05/06/business/facebook-bends-the-rules-of-audience-engagement-to-its-advantage.html?ref=business&_r=1.

[55] *See* Jack Marshall, *Facebook Wants to Help Sell Every Ad on the Web*, May 27, 2016, Wall St. Journal, http://www.wsj.com/articles/facebook-wants-to-help-sell-every-ad-on-the-web-1464321603.

least not yet.[56] Amazon's core business is retail, so data helps it to better tailor and target offerings. It does not share much of its customers' data with others.[57] Apple's core business is hardware like the iPhone, but it also makes a significant amount of money by leveraging the popularity of those devices and serving as a middleman that profits from the apps that run on its devices (Apple takes a percentage of revenues from app developers) and the services that consumers use on them (*e.g.,* it takes a cut of every transaction made on iTunes). Its devices do collect a lot of personal information, which it uses to help refine its products and make them more useful to consumers; it does not use that information to target ads.[58]

Data brokers like Acxiom have long been major players in the data collection business, working behind the scenes, and unbeknownst to consumers, to build and sell detailed profiles of consumers to an array of customers like banks, car companies, and retailers.[59] Hundreds of smaller firms also track users online in an attempt to gather and build similar profiles. Indeed, at any one time dozens of firms track consumers as they surf the Web, following their activities by surreptitiously attaching cookies and other bits of software to create a trail of data that they can collect and somehow monetize.[60]

2.3 *The Narrow Role of ISPs in the Data Collection Universe*

Within this world of data collection and monetization, ISPs play a very small role. Because consumers' online activities increasingly span multiple devices and locations, it is nearly impossible for a single ISP to glean as much information about a particular user's online behavior as, say, Google.[61] In addition, more and more data that flows over broadband networks is being encrypted, a dynamic that greatly limits the visibility an ISP might have into a customer's usage data.[62] Moreover, even though some ISPs use customer data to develop and market ancillary services, the financial growth of these companies remains almost exclusively tied to subscription fees for Internet access, video and telephone service, not advertising revenue.

---

[56] *See, e.g.,* Kate Kaye, *Why Can't Amazon and Apple Catch a Break on Madison Ave?*, Feb. 18, 2014, AdAge, http://adage.com/article/digital/amazon-apple-catch-a-break-madison-ave/291724/.

[57] *Id.*

[58] *See, e.g.,* Mark Hachman, *The Price of Free: How Apple, Facebook, Microsoft and Google Sell You to Advertisers*, Oct. 1, 2015, PC World, http://www.pcworld.com/article/2986988/privacy/the-price-of-free-how-apple-facebook-microsoft-and-google-sell-you-to-advertisers.html.

[59] *See, e.g.,* Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, June 16, 2012, N.Y. Times, http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=1.

[60] For an in-depth overview of an array of tracking activities, *see What They Know,* Wall St. Journal (series), http://www.wsj.com/public/page/what-they-know-digital-privacy.html.

[61] *See generally Swire Study.*

[62] *Id.*

Over time, though, ISPs appear likely to explore online advertising as a way to generate new revenues, but even then their market share and ability to gather data on a large scale – *i.e.,* across multiple networks, devices, services, and location – will be limited and greatly overshadowed by the efforts of incumbent companies like Facebook.[63] Such additional revenue streams, though, may prove vital to supporting continued investment in broadband infrastructure.[64] As such, foreclosing exploration of these new lines of business could very well chill investment and slow deployment of broadband networks.

3. ADDITIONAL INADEQUACIES OF THE FCC PROPOSAL

In addition to the fact that the proposed rules neither reflect the true nature of the data collection universe nor appreciate the significant power over consumer information wielded by firms other than ISPs, the Commission's proposed rules include several other troubling attributes that, if implemented, would harm consumers and the innovative health of the ecosystem. These harms include: (1) negative impacts on the "virtuous cycle," in particular the likelihood of depressed investment in networks and less robust use of online services by consumers; and (2) the creation of an inefficient patchwork of privacy rules that would leave many questions unanswered and create opportunities for bad behavior by edge firms. These are explored in turn below.

3.1 *Likely Negative Impacts on the Broadband Ecosystem*

In its 2015 Open Internet order, the FCC sought to justify implementation of onerous net neutrality rules for ISPs and reclassification of broadband as a telecommunications service as vital to furthering the "virtuous cycle."[65] This conception of the broadband ecosystem, first set forth in the National Broadband and then formally adopted by the Commission in its 2010 Open Internet order, describes the relationship between innovation and investment as one where "innovations at the edges of the network enhance consumer demand, leading to expanded investments in broadband infrastructure that, in turn, spark new innovations at the edge."[66] In other words, the Commission subjectively views edge providers as the critical driver of progress in the ecosystem – anything that undermines efforts at the edge will have knock-on effects in other segments of the ecosystem.[67] Thus the ability to communicate and interact with end-users in an unimpeded manner is of paramount importance to the FCC – in its view, broadband networks ought to only be

---

[63] *See, e.g., Moody's Says.*

[64] *Id.*

[65] *See Protecting & Promoting the Open Internet*, Report & Order on Remand, Declaratory Ruling, & Order, 30 FCC Rcd 560, at ¶ 2, GN Docket 14–28 (rel. March 12, 2015) ("*2015 Open Internet Order*").

[66] *Id.* (citing *Verizon v. FCC*, 740 F.3d 623, 659 (D.C. Cir. 2014) (striking down many aspects of the FCC's 2010 Open Internet order but accepting its "cycle" rationale)).

[67] *See, e.g., id.* at ¶ 83.

passive conduits through which edge providers interact with consumers.[68] (Interestingly, in the instant proposal, the Commission only cites to the cycle once, linking its proposed rules in a rather perfunctory manner to the "potential" for "boosting confidence in and therefore use of broadband services."[69])

What goes unmentioned in this framing of the ecosystem is that interactions between consumers and edge providers mostly revolve around the harvesting of customer data. Indeed, as noted in section 2, the business model of most edge providers depends not just on the ability to interact unimpeded with customers – it also relies on their ability to mine more and more granular information from users and monetize it by placing targeted advertisements. Although consumers are generally aware of the data collection tactics of edge firms[70] and place a relatively high value on their ability to receive free services in exchange for targeted advertising,[71] the possibility nevertheless exists that adoption of the FCC's proposed rules – as well as the failure to rationalize the many disparate sets of privacy rules that exist and reconcile competing regulatory mandates of agencies like the FCC and FTC – could undermine consumer demand for online services by allowing for and encouraging more intrusive data collection practices by edge providers to emerge unabated.

These are not hypothetical concerns. As discussed above, edge providers are engaged in a never-ending battle for data supremacy. For business reasons, their tactics are becoming increasingly opaque vis-à-vis the range of information being collected and how that data is used.[72] The rise of artificially intelligent algorithms that can adapt in real-time as new information is fed in, the emergence of a universally connected "Internet of things," and an overall explosion of digital data all raise by orders of magnitude the amount of information that is likely to be collected by edge providers. At some point, as consumers become more aware of intrusive data collection techniques, they will likely begin to care about the lengths to which a company is tracking them[73] – *i.e.,* whether they consider those methods

---

[68] The undersigned respectfully disagree with this view of the ecosystem and urge adoption of a more expansive and realistic conception of this space, one that reflects the increasing convergence of different segments and business models and that acknowledges the importance of fostering more intelligence at the core of networks – including the ability to prioritize traffic and engage in related pro-consumer business model experimentation – as well as at the edge.

[69] *NPRM* at ¶ 309.

[70] *See generally Privacy and Information Sharing.*

[71] *See* Press Release, *Zogby Poll: Americans Say Free, Ad-Supported Online Services Worth $1,200/Year; 85% Prefer Ad-Supported Internet to Paid*, May 11, 2016, PR Newswire, http://www.prnewswire.com/news-releases/zogby-poll--americans-say-free-ad-supported-online-services-worth-1200year-85-prefer-ad-supported-internet-to-paid-300266602.html (reporting on the findings of a recent consumer poll regarding how much consumers value their ability to access free online services).

[72] *See, e.g.,* BLACK BOX SOCIETY (describing many data gathering practices as occurring in black boxes that are designed to avoid close scrutiny).

[73] Survey data from a range of entities indicate that there are numerous lines that consumers wish edge providers would not to cross when it comes to privacy-related concerns. For a recent example, *see The State*

to be truly "creepy"[74] – or the ways in which a company encourages them to engage in socially unacceptable behavior so they can harvest more information.[75] Recent survey data supports this general dynamic: even though "only 3 in 10 Americans understand[] how companies share their personal information…89% [of consumers report] avoiding companies they don't believe protect their privacy and 74% of those who worry about their privacy limit[ed] their online activity in the last 12 months due to their concerns."[76]

Unfortunately, the relative laxity with which edge providers are regulated in the online privacy context – in an *ex post* and largely ad hoc manner by the FTC – creates incentives for firms to be even more clandestine with respect to their data collection methods.[77] Waiting for harms to occur in a "black box society" and in a world where consumers aren't aware of the full extent to which an edge firm gathers and uses its data risks a race to the bottom in terms of further privacy intrusions that are overlooked or dismissed by regulators as "business as usual." If and when consumers do catch on and begin to care, though, there is a good chance that they will pull back from using certain services, thereby undermining the virtuous cycle, a dynamic the FCC itself predicted in its 2015 Open Internet order[78] and the National Broadband Plan.[79]

The likelihood of direct negative impacts on ISP investment are also real. The imposition of an opt-in framework for ISPs would greatly impede their ability to generate new revenue streams stemming from digital advertising and related efforts. Even though ISPs don't currently engage in much digital advertising based on data collected from users, they will likely begin to explore these business models "as the old guard ecosystem evolves to

---

of Online Privacy 2016, Jan. 28, 2016, TRUSTe Privacy Blog, http://www.truste.com/blog/2016/01/28/state-online-privacy-2016/ ("*State of Online Privacy 2016*").

[74] *Theory of Creepy.*

[75] The consumer pushback against a device like Google Glass is instructive. For an overview, *see* Jake Swearingen, *How the Camera Doomed Google Glass*, Jan. 12, 2015, The Atlantic, http://www.theatlantic.com/technology/archive/2015/01/how-the-camera-doomed-google-glass/384570/.

[76] *State of Online Privacy 2016.*

[77] *See, e.g.,* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 352-354 (2016) (highlighting the consumer threats arising from the "bait and switch" practices of edge providers like Facebook and Google, wherein a "website…lures consumers with various free services or other promises but…later switches and adopts privacy-invasive practices" [citations omitted]).

[78] *2015 Open Internet Order* at ¶ 464 ("We find that if consumers have concerns about the privacy of their personal information, such concerns may restrain them from making full use of broadband Internet access services and the Internet, thereby lowering the likelihood of broadband adoption and decreasing consumer demand." [citations omitted]).

[79] *See Connecting America: The National Broadband Plan*, at 53, FCC (2010), http://download.broadband.gov/plan/national-broadband-plan.pdf ("...privacy concerns can serve as a barrier to the adoption and utilization of broadband").

become more competitive."[80] If adopted, though, the FCC's rules will likely hamper the ability of ISPs to "compete with digital advertisers such as Facebook and Google."[81] Such an outcome would be contrary to FCC policy vis-à-vis broadband because deployment of new networks – and investment generally – will stall. And such an outcome will be bad for consumers.

3.2 *Additional Concerns & Unanswered Questions*

Ongoing and emerging trends in data collection, many of which were discussed above, make clear that the online experience for consumers has long been managed and shaped by external forces. Indeed, competition among "edge providers" for data supremacy has created a dynamic where nearly every aspect of a consumer's Internet usage is fodder for digital advertising. It is thus unfortunately ironic that on the open Internet, users are anything but free. Rather, they are pawns in a game dominated by edge providers that revolves around capturing and monetizing as much personal information as possible. Perhaps most incredible is that users are largely powerless to alter this dynamic because they are constrained in their ability to know exactly which entities are following them, what kind of information is being gathered, and the ways in which their data is being used. Compounding this situation is the fragmented nature of privacy rules, rights, and "protections," sowing confusion among consumers and increasing a feeling of helplessness as they exchange more data and personal information for free services.[82]

There are many more privacy questions than answers at this point in time. These questions are fundamental and include the extent to which consumers have any rights at all to know more about their data. There are unanswered questions about the details of which online uses generate which kinds of information, where it goes, and who profits from it. Questions linger about whether users can opt into or out of tracking, about whether they have any ownership rights in their data, and about whether they can otherwise exert any control over their personal information. The FCC's privacy proposals would only further fracture this already uncertain regime at a time when more cohesion is needed, an outcome that could undermine investment in broadband services (see above).

In short, implementing the privacy framework proposed by the Commission would not address, even in an incremental manner, the most pressing questions and issues regarding online privacy and consumer empowerment. By its terms, the proposed framework would only be applicable to a small and, in the grand scheme, relatively innocuous set of actors in the data collection context. Indeed, there is little evidence offered by the FCC or any entity

---

[80] *See FCC's Broadband Privacy Proposal Credit Negative for Linear TV and Wireless Providers,* March 14, 2016, Moody's Investor Service, http://www.netcompetition.org/wp-content/uploads/FCC%E2%80%99s-broadband-privacy-proposal-credit-negative-for-linear-TV-and-wireless-providers.pdf.

[81] *Id.*

[82] *See, e.g., Privacy and Information Sharing* (providing insights into consumer attitudes towards such quid pro quo).

supportive of its proposals that even the most basic queries and concerns stemming from the enormous power over personal information wielded by edge entities like Google, Facebook, and Acxiom would be addressed – directly or indirectly – under this framework. Indeed, the FCC's proposed privacy rules would hinder much needed progress toward:

- Harmonizing the standards by which privacy policies are developed, maintained, updated, and communicated to end-users, including whether and to what extent consumers can opt into or out of services provided by all entities competing in the ecosystem – ISPs, content producers, data brokers, search engines, social media sites, and device manufacturers, among many others.

- Developing and enforcing uniform yet flexible standards to guide the dissemination of baseline information about the data collection methods used by firms competing in the ecosystem: *e.g.,* how data is collected, stored, analyzed, protected, sold, and monetized. Flexibility is important to ensuring that regulators are able to adapt rules to new collection techniques that might emerge.[83]

- Protecting consumers against potential abuses of their data. For example, there are many concerns around the ability of companies like Google and other large data aggregators to extrapolate personal details from online behavior (*e.g.,* purchases and search queries) and in-home interactions with devices like Home and Echo.[84] There are also significant concerns that such "big data" practices might "encod[e] discrimination in automated decisions," a dynamic that would disproportionately impact minorities and historically marginalized communities more than others.[85]

- Providing recourse in the event that a device or service enabled by a broadband connection – like Amazon Echo, a smart TV, or a microphone in a

---

[83] For an overview of an emerging class of post-cookies data collection techniques, *see* Jules Polonetsky and Stacey Gray, *Cross Device: Understanding the State of State Management*, Future of Privacy Forum (Nov. 2015), https://fpf.org/wp-content/uploads/2015/11/FPF_FTC_CrossDevice_F_20pg-3.pdf.

[84] For an example of an especially personal intrusion, *see* CHARLES DUHIGG, HABIT: WHY WE DO WHAT WE DO IN LIFE AND BUSINESS 182-212 (2012) (describing the data collection and analytical methods of Target and how it was able to target pregnancy- and baby-related ads to women it predicted were pregnant based on their in-store and online purchases).

[85] *See Big Data: Seizing Opportunities, Preserving Values*, Executive Office of the President (May 2014), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf. *See also Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, Executive Office of the President (May 2016), https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

smartphone – records and transmits to third-parties more information than a consumer wants or is aware of.[86]

The above is just a representative sampling of the unanswered questions, lingering consumer concerns, and potential enforcement gaps that would remain if the FCC moves forward with its privacy proposal. In short, the FCC's rules as currently structured would accomplish little vis-à-vis protecting consumer privacy or enshrining basic yet generally applicable privacy rights.

4. A MORE PRO-CONSUMER AND PRO-PRIVACY PATH FORWARD

Given the many inadequacies of the present proposal and the likelihood of consumer harm if implemented, it is respectfully suggested that the Commission pursue a different course of action. There are several related elements of this alternative path forward; these are discussed in turn below.

First, if the FCC's decision to reclassify broadband as a telecommunications service is upheld, then it should forbear from section 222 unless and until there are *actual* violations or harmful practices that require action. The NPRM fails to include any compelling or real examples of consumer harm stemming from ISP data collection practices; instead, the proposed rules are grounded in *hypothetical* bad behavior. Opting to forbear, though, would harmonize the Commission's approach, at least in spirit, with the FTC's *ex post* regime for policing data collection practices that are deemed "unfair or deceptive."[87] In addition, it would align with the Commission's case-by-case approach for monitoring harm that might run afoul of its Open Internet rules.[88] Indeed, electing to follow this path would provide much-needed guidance about how the Commission plans to operationalize its very broad General Conduct Standard.[89] Of course, if reclassification is not upheld in whole or in part – *i.e.,* if any element of the Open Internet order is struck down or remanded for further consideration – then the Commission should immediately pause this rulemaking until there

---

[86] *See, e.g., Goodbye Privacy* (noting such concerns stemming from use of Amazon's Echo); Julia Angwin, *Own a Vizio Smart TV? It's Watching You*, Nov. 9, 2015, Pro Publica, https://www.propublica.org/article/own-a-vizio-smart-tv-its-watching-you (reporting that "Vizio's Smart TVs track your viewing habits and share it with advertisers, who can then find you on your phone and other devices…The tracking — which Vizio calls "Smart Interactivity" — is turned on by default for the more than 10 million Smart TVs that the company has sold. Customers who want to escape it have to opt-out."); Stacey Gray, *Always On: Privacy Implications of Microphone-Enabled Devices*, Future of Privacy Forum (April 2016), https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf.

[87] *See, e.g., NPRM* at ¶ 8.

[88] *2015 Open Internet Order* at ¶¶ 21, 138 (describing the so-called General Conduct Standard).

[89] *See, e.g.,* Kit Walsh, *Today's Net Neutrality Order is a Win, With a Few Blemishes*, March 12, 2015, EFF, https://www.eff.org/deeplinks/2015/03/todays-net-neutrality-order-win-few-blemishes (observing that the FCC's approach to applying its amorphous General Conduct Standard "could…lead to overreach, and will certainly lead to expensive litigation).

is further guidance from the courts or Congress about the appropriateness of treating broadband as anything but an information service.[90]

Second, after forbearing, the FCC must recognize and appreciate the many risks inherent in creating a bifurcated digital privacy protection framework. Even though the FCC and FTC have an MOU outlining how the two agencies will work together to enhance consumer protection online,[91] there remains significant concern that maintaining two disparate privacy regimes will "confuse all but the savviest consumers" and ultimately "do little to promote the cause of "privacy.""[92] The best way to assure clarity and consistency across the ecosystem is for the FCC to join the FTC and other entities in calling on Congress to clarify:

> (1) *The proper regulatory classification of broadband.* As part of a long overdue update of the nation's communications laws, Congress must settle once and for all that it never intended for broadband to be regulated as a common carrier service. Doing so would not only bolster regulatory certainty and investment in broadband services – it would also bring broadband back within the regulatory orbit of the FTC, thereby creating much-needed consistency in the monitoring and enforcement of digital privacy intrusions.
>
> (2) *The full scope of consumer rights vis-à-vis online privacy and digital data collection.* There have been numerous efforts in recent years – by the FTC,[93] the Department of Commerce,[94] and the White House,[95] among many other

---

[90] The "information service" designation and the corresponding minimalist regulatory framework that was developed as a result played a critical role in supporting broadband investment, deployment, and innovation. Reclassifying broadband as a "telecommunications service" and regulating it as a common carrier service reverses the regulatory dynamic and threatens future investment by ISPs. For an overview of the importance of regulatory minimalism stemming from the information service designation, *see* Charles M. Davidson & Michael J. Santorelli, *Broadband, The States & Section 706: Regulatory Federalism in the Open Internet Era,* 8 Hastings Science & Technology Law Journal ___ (forthcoming 2016), http://www.nyls.edu/advanced-communications-law-and-policy-institute/wp-content/uploads/sites/169/2013/08/Davidson-Santorelli-706-The-States-February-2016.pdf. For an overview of likely harms to ISP investment resulting from reclassification, *see* Kevin A. Hassett and Robert J. Shapiro, *The Impact of Title II Regulation on Internet Providers and Their Capital Investments*, Sonecon (Nov. 2014), http://www.sonecon.com/docs/studies/Impact_of_Title_II_Reg_on_Investment-Hassett-Shapiro-Nov-14-2014.pdf.

[91] *See FCC-FTC Consumer Protection Memorandum,* FCC (Nov. 2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-336405A1.pdf.

[92] *See* Jon Leibowitz and Jonathan Nuechterlein, *The New Privacy Cop Patrolling the Internet*, May 10, 2016, Fortune, http://fortune.com/2016/05/10/fcc-internet-privacy/.

[93] *FTC Privacy Report.*

[94] *See Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, Green Paper, Internet Policy Task Force, U.S. Dept. of Commerce (Dec. 2010), https://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf.

entities – to articulate, in some form or another, a consumer "bill of rights" vis-à-vis online privacy. Congressional action to codify some or all of these principles would help to identify the basic contours of 21st century privacy protections that consumers can expect to be upheld whenever they go online.

(3) *The agency – the FCC, FTC, or some other entity – that will be the primary cop on the privacy beat.* To prevent against further or future bifurcation of privacy regimes, Congress must make clear which agency has authority to implement and enforce privacy rules and standards for digital information.

Third, if the FCC insists on pursuing its current proposal, then it should expand the reach of its rules to encompass *all* firms in the ecosystem. This will assure parity, consistency, and a more aggressive "cop on the beat." This could be done by grounding its rules in section 706 of the Telecommunications Act. Some have noted that section 706 could be easily extended to reach "edge providers;"[96] such action in the privacy context makes sense because, as discussed at length above, protecting consumers from nefarious data collection and monetization practices is essential to furthering the "value cycle."

5. CONCLUSION

For the many reasons discussed in these comments, the undersigned respectfully call on the FCC to reevaluate its proposed privacy rules and defer to Congress to develop the kind of comprehensive and consistent digital privacy framework that 21st century consumers need and deserve.

Respectfully submitted,

/s/ Charles M. Davidson
Charles M. Davidson, Director
ACLP at New York Law School
185 West Broadway
New York, NY 10013

/s/ Michael J. Santorelli
Michael J. Santorelli, Director
ACLP at New York Law School
185 West Broadway
New York, NY 10013

Submitted: May 27, 2016

---

[95] *See Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, The White House (Feb. 2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[96] *See, e.g.,* Daniel T. Deacon, *Common Carrier Essentialism and the Emerging Common Law of Internet Regulation,* 67 Admin. L. Rev. 133, 173 (2015) ("…there is no reason that [the] FCC could not use its § 706 power instead to regulate edge providers directly, at least as long as it could tell a credible story regarding why such regulation enabled innovation at the edge (in turn spurring consumer demand for broadband and, with it, broadband infrastructure deployment, under the "virtuous cycle" theory)." [citations omitted]).